ad. 17

$C_8 = (\{0,1,2,3,4,5,6,7\}, +_8)$

$H \leq G \iff$ 1) $e \in H$ 2) $\forall a,b \in H \; a +_8 b \in H$ 3) $\forall a \in H \; a^{-1} \in H$

Niech $H \leq G$

stąd $0 \in H$, $(\{0\}, +_8)$ $(C_8, +_8)$

z 2) $1 \in H \Rightarrow 1+1 \in H \Rightarrow \dots \Rightarrow \langle 1 \rangle = C_8$

$3 \in H \Rightarrow 1 \in H$

$2 \in H \Rightarrow 4 \in H \wedge 6 \in H$: $(\{0,2,4,6\}, +_8)$

$(\{0,4\}, +_8)$

$\boxed{4=4}$

ad. 11

1) $H = \{0,3\}$ $G = C_6$

$0 +_6 H = 3 +_6 H = \{0,3\} = [0]_H$

$1 +_6 H = 4 +_6 H = \{1,4\} = [1]_H$

$2 +_6 H = 5 +_6 H = \{2,5\} = [2]_H$

6) $H = \{0, \alpha\}$, $G = D_8$

L: $[0]_{\sim_H} = \{0, \alpha\} = [\alpha]_{\sim_H}$ P: $[0]_{\sim_H} = \{0,\alpha\} = [\alpha]_{\sim_H}$

$[r]_{\sim_H} = \{r, r^3\alpha\}$ $[r]_{\sim_H} = \{r, r\alpha\}$

$[r^2]_{\sim_H} = \{r^2, r^2\alpha\}$ $[r^2]_{\sim_H} = \{r^2, r^2\alpha\}$

$[r^3]_{\sim_H} = \{r^3, r\alpha\}$ $[r^3]_{\sim_H} = \{r^3, r^3\alpha\}$

ad. 16

a) $G = \langle g \rangle$ $|G| = m$

tw. $\langle g^k \rangle = \langle g^{\text{NWD}(k,m)} \rangle$ $\langle g^k \rangle = \langle \dots, g^k, g^{-k}, g^{2k}, \dots \rangle$
$k = mq$

$\langle g^m \rangle = \langle e, g^m, g^{-m}, \dots, g^k, \dots \rangle$

(2°)

$\langle g^m \rangle \subseteq \langle g^k \rangle \Rightarrow \langle g^m \rangle = \langle g^k \rangle$ $\langle g^k \rangle \leq \langle g^m \rangle \dots$

$m = kx + my$ | $x, y \in \mathbb{Z}$

$g^{kx+my} = g^m$

$g^{kx} g^{my} = g^m$

$(g^k)^x = g^m$

b) $|G| = m$ $d | m$

tw. Istnieje jedna podgrupa mocy d.

$\text{ord}(g_1) = \text{ord}(g_2) = d$. $\langle g_1 \rangle = \langle g_2 \rangle$

$|\langle g_1 \rangle| = \frac{n}{\text{nwd}(d,m)}$ $|\langle g \rangle| = \frac{n}{\text{nwd}(g,n)} = \frac{n}{\text{nwd}(g_1,g_2)}$

1° Jeśli $d | m$

$\operatorname{ord}(g^{\frac{m}{d}}) = d$

2° $k \nmid m$ $\quad$ z 1 faktu

$\underbrace{\langle g^k \rangle = \langle g^{\mathrm{nwd}(k,m)} \rangle}$

$\underbrace{k | m}$

$\operatorname{ord} = k \neq d$

to nie jest rzędu d, bo to jest tego samego rzędu, co k, bo to jedna z grup, które wcześniej wymieniłem.

ad. 18

p, q - pierwsze, $p \neq q$.

Znajdź C_p, C_q, C_{pq} $\quad$ g - generator C_{pq}

$\langle g^k \rangle = \langle g^{\mathrm{nwd}(m,k)} \rangle$

$\langle a_1, \dots, a_k \rangle = \langle b_1, \dots, b_k \rangle$ Jeżeli weźmiemy $H < C_{pq}$: H jest cykliczna. $H = \langle g^k \rangle = \langle g^{\mathrm{nwd}(k,pq)} \rangle$

Wystarczy $k | pq$

1) C_p

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \langle 0, 1, \dots, p-1 \rangle$

2) C_{pq} $\quad pq \to \langle 0 \rangle$

$q \to \langle p, 2p, \dots, p(q-1) \rangle$

$p \to \langle q, \dots, q(p-1) \rangle$

$1 \to C_{pq}$

Wystarczy sprawdzić wszystkie dzielniki pq.

~~$C_{pq} \langle 1, 2, \dots, pq \rangle$~~

~~C_{pq} ...~~ -

Podgrupy C_n:

$\{ \langle k \rangle : k | n \}$

ad. 19

$\left\{ \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} : k \in \mathbb{Z} \right\}$ $GL(2, \mathbb{R})$

$\forall_{m,n \in \mathbb{Z}} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & m+n \\ 0 & 1 \end{bmatrix}$ $\quad m+n \in \mathbb{Z}$

$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ $\quad \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$ $\quad g = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$